논문 17-42-07-07 The Journal of Korean Institute of Communications and Information Sciences '17-07 Vol.42 No.07
https://doi.org/10.7840/kics.2017.42.7.1352

물리계층 보안을 향상시키기 위한 파워 분할 기반 릴레이

이 기 송•, 최 현 호°

Power Splitting-Based Relaying for Improving Physical Layer Security

Kisong Lee•, Hyun-Ho Choi°

요 약

본 논문에서는 발신원로부터 전송되는 신호로부터 에너지 하베스팅이 가능한 무전원 릴레이가 존재하는 2-hop 네트워크에서 물리계층 보안을 최대화하기 위한 파워 분할 기반 relaying 기법을 제안한다. 시뮬레이션을 통해 제안 방안이 도청자의 도청을 막아 최적의 보안 용량을 달성함을 보이고, 기존 방안과의 비교를 통해 제안 방안의 우수성을 보인다.

Key Words : Energy Harvesting, Relay Protocol, Power Splitting, Secrecy Capacity, Physical Layer Security

ABSTRACT

In this paper, we propose a power splitting-based relaying protocol for maximizing a physical layer security in 2-hop networks where a batteryless relay can harvest energy from the signal transmitted by a source. Through simulations, it is demonstrated that the proposed scheme achieves an optimal secrecy capacity by preventing the eavesdropper from overhearing, and outperforms the conventional schemes.

Ⅰ. 서 론

최근 무선 네트워크에서는 센서의 전원 부족 문제를 해결하기 위한 기술에 대한 요구가 커지고 있다. 이에 대한 요구에 따라, 기존의 버려지는 RF 신호로부터 전력을 수집하여 활용하는 RF 에너지 하베스팅(Energy harvesting) 기술에 대한 관심이 높아지고 있다[1-3]. [1]에서는 RF 신호를 이용하여 정보와 전력을 동시에 수신하기 위한 적응적 파워 분할 기법을 제안하였다. [2]에서는 무전원 노드를 이용한 에너지 하베스팅 기반의 릴레이 프로토콜을 제안하였다. (3)에서는 정보와 전력 동시 전송을 최대화하기 위한 자원할당 방안을 제안하였다. 뿐만 아니라, 최근 수많은 통신 노드가 사용되는 사물인터넷 환경이 구현됨에 따라, unlicensed 사용자에게 원하지 않게 전달될 수 있는 정보 유출 문제 해결이 상당히 중요한 이슈로 떠오르고 있다[4,5]. [4]에서는 릴레이가 존재하는 분산 네트워크 환경에서 정보 보안을 최대화하기 위한 협력적 파워 할당 기법이 제안되었다. 또한, [5]에서는 다수의 릴레이가 존재할 때 정보 보안을 최대화하기 위한 최적의 릴레이 선택 방안이 연구 되었다.

본 논문에서는, 무전원 릴레이(Relay)가 존재하는 분산 네트워크 환경에서 네트워크의 물리계층 보안(Physical layer security)을 최대화하고자 한다. 릴레이는 발신원(Source)로부터 전송되는 신호로부터 에너지를 하베스팅 할 수 있으며, 이 전력을 이용하여 목적지(Destination)에 신호를 전달한다. 이때, 릴레이에서 전송한 신호는 목적지 주변의 도청자(Eavesdropper)에서 도청이 가능하다. 이러한 환경에서 발신원에서 전달된 신호가 도청자에 도청 당하지 않고 안전하게 목적지에 전달될 수 있도록, 네트워크 보안 용량(Secrecy capacity)을 최대화 할 수 있는 최적의 파워 분할 기반 relaying 기법을 제안 한다. 또한, 다양한 시뮬레이션 환경에서 기존 방안과의 비교를 통해 제안 방안의 우수성을 검증한다.

※ 이 논문은 2015 및 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No. 2015R1C1A1A01051747, No. 2016R1C1B1016261)
• First Author : Kunsan National University, Department of Information and Telecommunication Engineering, kslee@kunsan.ac.kr, 정회원
° Corresponding Author : Hankyong National University, Department of Electrical, Electronic and Control Engineering, hhchoi@hknu.ac.kr, 정회원
논문번호 : KICS2017-05-156, Received May 26, 2017; Revised June 21, 2017; Accepted July 4, 2017

Ⅱ. 파워 분할 기반 릴레이 기법

본 논문에서는 그림 1에서처럼 발신원, 릴레이, 목적지, 도청자가 존재하는 2-hop 네트워크를 고려한다. source-to-relay, relay-to-destination, relay-to-eavesdropper 간의 채널을 각각 h_{sr}, h_{rd}, h_{re}로 정의하고, 각 채널은 independent and identically distributed (i.i.d.) 플랫 페이딩 채널이라 가정한다. source-to-destination, source-to-eavesdropper, and destination-to-eavesdropper 간의 direct link는 없다고 가정한다[2,4]. 각 노드에는 $n \sim CN(0,\sigma^2)$의 동일한 Additive White Gaussian Noise가 존재한다고 가정한다. 본 논문에서 고려하고 있는 파워 분할 기반 릴레이 프로토콜(Power splitting-based relaying protocol)은 전체 블록 시간 T 동안 2-phase로 이루어져 있다. 먼저, T/2의 시간에 해당하는 phase 1에서는 발신원이 릴레이에게 신호 s를 전송한다. 이때 릴레이는 무전원 노드이므로, 발신원으로부터 받은 신호 중 ρ 에 해당하는 파워를 이용하여 에너지 하베스팅을 하고, $1-\rho$에 해당하는 파워를 이용하여 신호를 수신한다[1,2]. 나머지 T/2의 시간에 해당하는 phase 2에서 릴레이는 phase 1에서 충전한 파워를 이용하여 Amplify-and- forward (AF) 기법을 이용하여 목적지에서 신호를 전달한다. 이때 전달된 신호는 도청자에게도 전달이 되어 도청이 된다.

Phase 1에서 릴레이가 수신하는 신호 y_r은 다음과 같이 표현이 가능하다.

$$y_r = \sqrt{(1-\rho)P_S}h_{sr}s + n. \tag{1}$$

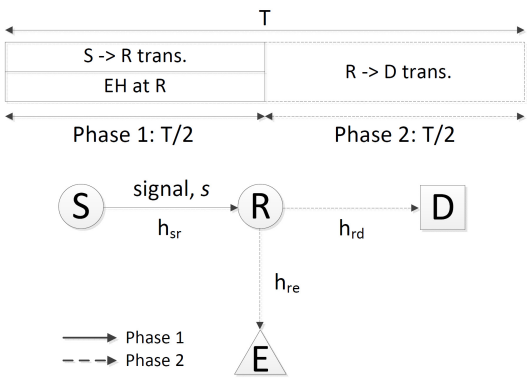

그림 1. 에너지 하베스팅이 가능한 파워 분할 기반 relaying 시스템 모델
Fig. 1. System model of power splitting- based relaying with energy harvesting

수식 (1)에서 P_S는 발신원의 전송 파워이며, 신호 s는 $E[|s|^2]=1$의 정규화 된 파워를 갖는다. 반면에 릴레이에서 하베스팅된 에너지는 다음과 같다.

$$E_h = \frac{T\eta\rho P_S|h_{sr}|^2}{2}. \tag{2}$$

여기서 η는 에너지 변환 효율이다.

Phase 2에서 릴레이는 하베스팅한 에너지 E_h를 이용하여 수신 신호를 증폭한다. 릴레이에서 전송되는 신호 x_r은 다음과 같다.

$$x_r = \frac{\sqrt{P_r}\,y_r}{\sqrt{(1-\rho)P_S|h_{sr}|^2+\sigma^2}}. \tag{3}$$

여기서 릴레이가 전송에 사용하는 파워 P_r은 수식 (4)로 표현될 수 있다.

$$P_r = \frac{E_h}{T/2} = \eta\rho P_S|h_{sr}|^2. \tag{4}$$

또한, 목적지에서 수신되는 신호 y_d는 아래와 같이 표현된다.

$$\begin{aligned} y_d &= h_{rd}x_r + n \\ &= \frac{\sqrt{(1-\rho)P_SP_r}\,h_{sr}h_{rd}s + \sqrt{P_r}\,h_{rd}n}{\sqrt{(1-\rho)P_S|h_{sr}|^2+\sigma^2}} + n. \end{aligned} \tag{5}$$

반면, 도청자에서 도청되는 신호 y_e는 아래와 같이 표현된다.

$$\begin{aligned} y_e &= h_{re}x_r + n \\ &= \frac{\sqrt{(1-\rho)P_SP_r}\,h_{sr}h_{re}s + \sqrt{P_r}\,h_{re}n}{\sqrt{(1-\rho)P_S|h_{sr}|^2+\sigma^2}} + n. \end{aligned} \tag{6}$$

수식 (5)로부터 목적지에서의 signal- to-noise ratio (SNR)은 다음과 같이 표현된다.

$$\begin{aligned} \gamma_d &= \frac{(1-\rho)P_rP_S|h_{sr}|^2|h_{rd}|^2}{P_r|h_{rd}|^2\sigma^2+\sigma^2((1-\rho)P_S|h_{sr}|^2+\sigma^2)} \\ &= \frac{\eta\rho(1-\rho)P_S^2|h_{sr}|^4|h_{rd}|^2}{\eta\rho P_S|h_{sr}|^2|h_{rd}|^2\sigma^2+\sigma^2((1-\rho)P_S|h_{sr}|^2+\sigma^2)}. \end{aligned} \tag{7}$$

또한, 수식 (6)으로부터 도청자에서의 SNR은 다음과 같이 표현된다.

$$\gamma_e = \frac{(1-\rho)P_r P_S |h_{sr}|^2 |h_{re}|^2}{P_r |h_{re}|^2 \sigma^2 + \sigma^2((1-\rho)P_S |h_{sr}|^2 + \sigma^2)} = \frac{\eta\rho(1-\rho)P_S^2 |h_{sr}|^4 |h_{re}|^2}{\eta\rho P_S |h_{sr}|^2 |h_{re}|^2 \sigma^2 + \sigma^2((1-\rho)P_S |h_{sr}|^2 + \sigma^2)}. \quad (8)$$

결론적으로 γ_d와 γ_e로부터 네트워크의 보안 용량은 다음과 같이 목적지에서의 통신 용량과 도청자에서의 통신 용량의 차로 구할 수 있다[4,5].

$$C_S = \left[\frac{T}{2}\{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\}\right]^+. \quad (9)$$

수식 (9)의 C_S를 최대화 하는 ρ는 exhaustive search를 통해 찾을 수 있다.

Ⅲ. 시뮬레이션 결과

시뮬레이션에서는 $T = 1s$, Transmit SNR ($\frac{P_S}{\sigma^2}$)=83dB, m(Path-loss exponent)=2.7, $d_{sd} = 30m$, $\eta = 0.5$[3]로 가정하였다. 또한, 평균 1을 갖는 exponentially distributed random variable을 이용하여 채널을 생성하였다[1,2]. 시뮬레이션을 통해 각 채널 상황에서 C_S를 최대화 할 수 있는 최적의 ρ를 찾는 Optimal power splitting(OPS)과 채널 상황에 무관하게 일정한 ρ값을 사용하는 기존 방안의 성능을 비교하였다. 그림 2와 3에서는 채널 파라미터의 영향을 보기 위해 다음과 같은 3가지 경우에 대해 결과를 확인하였다; i) $d_{sr} = d_{rd} = 15m$, ii) $d_{sr} = 5m < d_{rd} = 25m$, iii) $d_{sr} = 25m > d_{rd} = 5m$.

그림 2는 파워 분할 비율에 대한 보안 용량을 보여준다. 여기서 $d_{re} = 15m$로 고정하였다. 각각의 경우에서 C_S는 ρ에 대해 concave한 형태를 지니며, 최적의 ρ값이 존재한다. 또한, d_{sr}이 작아질수록 최적의 ρ값이 커짐을 확인할 수 있다.

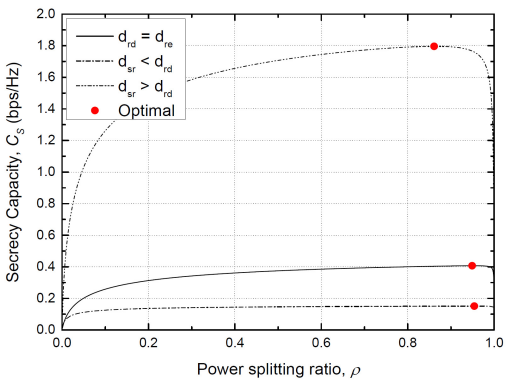

그림 2. 보안 용량 vs. 파워 분할 비율
Fig. 2. Secrecy capacity vs. Power splitting ratio

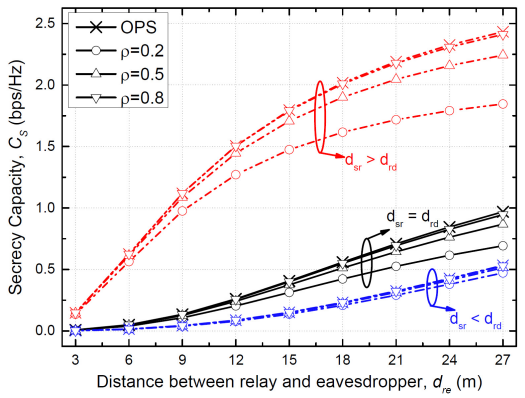

그림 3. 보안 용량 vs. 릴레이와 도청자 사이의 거리
Fig. 3. Secrecy capacity vs. Distance between relay and eavesdropper

그림 3은 릴레이와 도청자 사이의 거리에 대한 보안 용량을 보여준다. d_{sr}이 커질수록 C_S가 커짐을 확인할 수 있다. 또한, d_{re}가 커짐에 따라 도청자로 전달되는 신호의 크기가 현저히 줄어들고, 이에 따라 도청을 할 수 없게 되어 전 기법의 C_S가 향상된다. 뿐만 아니라, OPS가 일정한 ρ를 사용하는 기존 방안에 비해 크게 성능을 개선시킴을 확인할 수 있다.

Ⅳ. 결 론

본 논문에서는 발신원으로부터 전달되는 신호로부터 에너지 하베스팅이 가능한 무전원 릴레이가 존재하는 분산 네트워크에서 보안 용량을 최대화하기 위한 릴레이 프로토콜을 제안하였다. 발신원, 릴레이, 목적지, 도청자 등 4개의 노드가 존재하는 2-hop 네트워크 환경을 수식적으로 모델링하고, 보안 용량을 최대화 할 수 있는 최적의 파워 분할 비율을 찾았다. 시뮬레이션을 통하여 제안 방안이 기존 방안에 비해 보안 용량을 개선하여, 물리계층 보안을 향상시킬 수 있음을 확인하였다. 추후 연구로 최적의 파워 분할 비율을 수식적으로 도출하고, 실제 환경에서 릴레이의 에너지 하베스팅 가능성을 검증하고자 한다.

References

[1] L. Liu, R. Zhang, and K. Chua, “Wireless information and power transfer: a dynamic power splitting approach,” *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990-4001, Sept. 2013.

[2] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, “Relaying protocols for wireless energy harvesting and information processing,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, 2013.

[3] K. Lee, M. Kim, and D.-H. Cho, “Resource management for maximizing simultaneous transfer of information and power,” *J. KICS*, vol. 40, no. 8, pp. 1560-1566, Aug. 2015.

[4] K.-H. Park, T. Wang, and M.-S. Alouini, “On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sept. 2013.

[5] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical layer security in cooperative wireless networks,” *IEEE J. Sel. Topics Sign. Process.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.